



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/544,709	04/06/2000	Vipin Samar	OR99-17501	9115

51067 7590 09/02/2005

ORACLE INTERNATIONAL CORPORATION
c/o A. RICHARD PARK
2820 FIFTH STREET
DAVIS, CA 95616-2914

EXAMINER

HENEGHAN, MATTHEW E

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 09/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/544,709

Applicant(s)

SAMAR, VIPIN

Examiner

Matthew Heneghan

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 June 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6, 8-23, 25-40 and 42-55 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 8-23, 25-40 and 42-55 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 April 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 23 May 2005 has been entered.

2. In response to the previous office action, Applicant has amended claims 1, 18, 35, 52, and 55. Claims 1-6, 8-23, 25-40, and 42-55 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 2, 6, 8, 9, 11-13, 17-19, 23, 25, 26, 28-30, 34-36, 40, 42, 43, 45-47, 51-53, and 55 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,790,785 to Klug et al. in view of U.S. Patent No. 5,224,163 to Gasser et al.

As per claims 1, 2, 6, 8, 9, 11-13, 18, 19, 23, 25, 26, 28-30, 35, 36, 40, 42, 43, 45-47, and 55, the registration information processing system disclosed by Klug receives a password request (or sets up a new password for the user), authenticating it on behalf of the application, looks up the password for the application in the user registration information database (or creates it automatically or in cooperation with the user) and sends it to the application (see column 6, line 37 to column 7, line 60).

Klug does not disclose the authentication of the remote computer system based upon a chain of certificates and signatures.

Gasser discloses a system for delegating authorization wherein a workstation verifies a user, and then executes all transactions of behalf of the user using chains of signed certificates (see column 13, line 21 to column 14, line 18 and column 7, lines 29-48). Gasser further suggests that this is done because all systems on a network cannot be equally trusted and, because distributed networks often have a large number of network entities, it is generally desirable to organize the entities into manageable groups (see column 2, line 60 to column 3, line 1).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Klug by having the workstation execute transactions of behalf of the user using chains of signed certificates, as

disclosed by Gasser, as all systems on a network cannot be equally trusted and it is generally desirable to organize the entities into manageable groups.

As per claims 17, 34, and 51, the new password information can be created by the system in response to actions by the remote application (see column 11, lines 31-63).

As per claims 52 and 53, the user can retrieve id and password information for the application and send it back to the user (see column 13, lines 39-49).

3. Claims 1-6, 8, 9, 11-13, 15, 17-23, 25, 26, 28-30, 32, 34-40, 42, 43, 45-47, 49, and 51-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,790,785 to Klug et al. in view of U.S. Patent No. 5,224,163 to Gasser et al. further in view of U.S. Patent No. 5,611,048 to Jacobs et al. further in view of U.S. Patent No. 6,000,033 to Kelley et al.

As per claims 1-6, 8, 9, 11-13, 18-23, 25, 26, 28-30, 35-40, 42, 43, 45-47, 54, and 55, the registration information processing system disclosed by Klug receives a password request (or sets up a new password for the user), authenticating it on behalf of the application, looks up the password for the application in the user registration information database (or creates it automatically or in cooperation with the user) and sends it to the application (see column 6, line 37 to column 7, line 60).

Klug does not disclose the authentication of the remote computer system based upon a chain of certificates and signatures.

Gasser discloses a system for delegating authorization wherein a workstation verifies a user, and then executes all transactions of behalf of the user using chains of signed certificates (see column 13, line 21 to column 14, line 18 and column 7, lines 29-48). Gasser further suggests that this is done because all systems on a network cannot be equally trusted and, because distributed networks often have a large number of network entities, it is generally desirable to organize the entities into manageable groups (see column 2, line 60 to column 3, line 1).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Klug by having the workstation execute transactions of behalf of the user using chains of signed certificates, as disclosed by Gasser, as all systems on a network cannot be equally trusted and it is generally desirable to organize the entities into manageable groups.

Klug discloses the implementation of the registration system by using a platform-independent language, HTML (see column 4, lines 31-37), but does not explicitly disclose the use of platform-independent code.

Official notice is given that it is well-known in the art that the JAVA programming language, which is platform-independent, is incorporated into HTML in order to give increased programming flexibility, and that the use of certificate chains in JAVA applets is a well-known method for efficiently keeping track of trusted remote sites.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the system disclosed by Klug and Gasser using

JAVA, in order to give increased programming flexibility, and to use certificate chains in JAVA applets, in order to efficiently keep track of trusted remote sites.

Klug and Gasser do not disclose the use of location information in the authentication process over and above Gasser's certificate chains.

The remote password administration system disclosed by Jacobs authenticates users using node id's in addition to passwords (see column 9, line 66 to column 10, line 28). Jacobs further suggests that the criteria for valid passwords vary between security systems, and that it is important to coordinate passwords between local nodes and servers.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system disclosed by Klug and Gasser by authenticating users using node id's in addition to passwords, since criteria for valid passwords vary between security systems and it is important to coordinate passwords between local nodes and servers.

Klug, Gasser, and Jacobs also do not disclose the accessing of different passwords for different applications.

Kelley discloses a password retrieval system that may be used remotely (see column 6, lines 28-30) wherein different passwords for respective applications may be retrieved (see abstract) and further notes that this is necessary because different applications may have different naming conventions for their passwords (see column 1, lines 17-25).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to further modify the system disclosed by Klug, Gasser, and Jacobs by providing passwords on an application-by-application basis, as disclosed by Kelley, because different applications may have different naming conventions for their passwords.

As per claims 15, 32, and 49, Klug and Gasser do not disclose the storing of the password database separate from the password server.

Jacobs discloses the login information is stored in a separate database server apart from the mainframe (see abstract). Jacobs further suggests that this is to administrate and coordinate passwords across two or more security systems in a network (see column 2, lines 2-7).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to further modify the system disclosed by Klug, Gasser, Jacobs, and Kelley by storing login information in a separate database server apart from the mainframe, as disclosed by Jacobs, in order to administrate and coordinate passwords across two or more security systems in a network.

As per claims 17, 34, and 51, the new password information can be created by the system in response to actions by the remote application (see Klug, column 11, lines 31-63).

As per claims 52 and 53, the user can retrieve id and password information for the application and send it back to the user (see Klug, column 13, lines 39-49).

Art Unit: 2134

4. Claims 10, 14, 16, 27, 31, 33, 44, 48, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,790,785 to Klug et al. in view of U.S. Patent No. 5,224,163 to Gasser et al. further in view of U.S. Patent No. 5,611,048 to Jacobs et al. further in view of U.S. Patent No. 6,000,033 to Kelley et al. as applied to claims 1, 18, and 35, above, and further in view of U.S. Patent No. 5,623,637 to Jones et al.

Klug, Gasser, Jacobs, and Kelley do not disclose the storage of passwords on a removable medium, or the storage of the passwords in an encrypted manner, or authentication using smart cards or public keys.

As per claims 10, 27, and 44, the smartcard disclosed by Jones allows for the storage of public keys, in order to send secure transmissions to a remote receiving computer (see column 9, lines 38-47).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system disclosed by Klug, Gasser, Jacobs, and Kelley by storing public keys, as disclosed by Jones, in order to send secure transmissions to a remote receiving computer.

As per claims 14, 16, 31, 33, 48, and 50, the data storage card disclosed by Jones stores encrypted password values in a smartcard (see column 2, lines 30-43), and suggests that this is to allow the secure storage of private information in a compact easily transportable storage device, protected against unauthorized access if it is lost or stolen (see column 1, lines 61-67).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to further modify the system disclosed by Klug, Gasser, Jacobs, and Kelley by storing encrypted password values in a smartcard, as disclosed by Jones, in order to allow the secure storage of private information in a compact easily transportable storage device, protected against unauthorized access if it is lost or stolen.

Response to Arguments

5. Applicant's arguments, see Remarks, filed 23 May 2005, with respect to the rejections of the claims under 35 U.S.C. 102 and 103 have been fully considered and are persuasive in view of Applicant's amendments. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Gasser.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

P.O. Box 1450

Alexandria, VA 22313-1450

Or faxed to:

(571) 273-3800

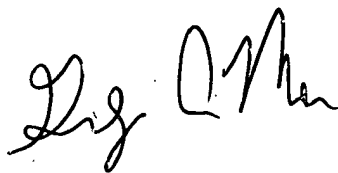
Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH



August 30, 2005



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100